APPLICATION

of

FRANK A. TRAYLOR, CHRISTOPHER S. DANG, PAUL A. BRILL,

AARON M. SWANSON

for

UNITED STATES LETTERS PATENT

on

SYSTEM FOR, AND METHOD OF, ENHANCING PUBLIC SAFETY ACTIVITY

Client ID/Matter No.: VISTK-64453

Sheets of Drawings: 11; Figures: 14

Express Mail Label No.: EV325905155US

[15101.1]

Attorneys
FULWIDER PATTON LEE & UTECHT, LLP
Howard Hughes Center
6060 Center Drive, Tenth Floor
Los Angeles, CA 90045

SYSTEM FOR, AND METHOD OF, ENHANCING PUBLIC SAFETY ACTIVITY

This invention relates to methods of forming and operating networks relating to public safety activity. The invention also relates to systems involving a network of groups and individuals for providing public safety activity.

BACKGROUND OF A PREFERRED EMBODIMENT OF THE INVENTION

Since the destruction of the World Trade Center in New York City on September 11, 2001, a great emphasis has been placed on increasing public safety. A separate Cabinet position designated as Secretary of Homeland Security has been created in the United States Government to deal with public safety. Large sections of different government agencies have been transferred to the Department of Homeland Security to deal with public safety. The Department of Homeland Security is now one of the largest departments in the United States Government.

The issues of dealing with public safety are quite complex. For example, even a relatively simple event such as the occurrence of a fire in a community may involve the fire department and, the police and hospital authorities in the community depending upon the severity of the fire. The fire department is of course involved in putting out the fire. The police department may be involved in directing traffic and in preventing looting. The hospital authorities may be involved if there are any injuries and if there are any burns in individuals. It would be desirable to have coordination between the different agencies such as the fire and police departments and the hospital authorities. If the fire is large, more than one fire department and more than one police department may be involved.

As another example, an act of terror may occur in a community. In that case, a number of different agencies may be involved. Some of these agencies may be national. The Federal Bureau of Investigations may be involved at the national level. State agencies dealing with safety and the state police may be involved. And, of course, local agencies such as local police may be involved. It would be desirable to have the agencies at the different governmental levels involved on a coordinated basis to investigate the act of terror from various aspects such as who perpetuated the act of terror, who helped the terrorists and who financed the terrorists. It would also be desirable to investigate what acts the terrorists are planning to perpetuate in the future and attempt to forestall these activities.

BRIEF DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

This invention provides a method of, and a system for, engaging in a public safety activity in which a plurality of resource groups may form a coordinated network at national, state and local levels in directing and implementing the public safety activity and in which a dynamic response group may be formed from individuals in the different resource groups and included in the network to enhance the operation of the network.

In a preferred embodiment of the invention, a hub involving a large geographical area (e.g. state) communicates with other hubs and with spokes involving smaller geographical areas within the hub area. Selective hubs and spokes form a network in which they communicate messages to one another to enhance a public safety activity. A dynamic response group formed from individuals in the spokes may also be included in the network. The communication between the hubs and the spokes may be voluntary and may occur through Radix switches which identify the sender and the recipient in the network, process the message and pass the processed message to the recipient. Each group or individual may be invited, or ask to be invited, into the network. Each group or individual may leave the network voluntarily or at the network's request. The groups and individuals act in the network on a coordinated basis to enhance the public safety activity.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic a block diagram showing (a) a map of the United States and a disposition of a plurality of Radix hubs in various sections of the United States and, as indicated by broad lines, a communication between the hubs and (b) a plurality of Radix spokes, each associated with an individual one of the hubs, and (c) as indicated by narrow lines, a communication between each of the hubs and the associated spokes with the hubs;

Figure 2 is a schematic diagram showing a Radix spoke in additional detail;

Figure 3 is a schematic diagram, primarily in block form, of a system including a Radix hub and agencies providing different types of communication with the Radix hub and including a Radix switch and a firewall between each agency and the Radix hub;

Figures 4a and 4b are schematic diagrams, primarily in block form, showing in additional detail the construction of one of the Radix switches and the relationship between the Radix switch and the agencies at the opposite ends of the Radix switch;

Figure 5 is another schematic diagram showing in additional detail, (a) one of the hubs and two (2) spokes associated with the hub and (b) a separate Radix switch between the spokes and the hub and also including a chart showing the relationship between the hub and the spokes and further including a response group formed from individuals within the spokes;

Figure 6 is a block diagram listing resource groups and a response group and showing on a screen different messages to two (2) of the individuals in the response group and certain parameters relating to the messages;

Figure 7 is a schematic diagram of a pane on the monitor for providing different responses to a message introduced to the screen in the monitor;

Figure 8 is a schematic diagram indicating how messages and attachments are sent by a sender to a recipient;

Figure 9 is a schematic diagram illustrating how attachments to a message are selected and sent with the message to a recipient;

Figure 10 is a schematic diagram showing different buttons capable of being actuated by a user and showing the different functions controlled by the actuation of the buttons;

Figure 11 is a schematic diagram indicating the status of an incoming message – for example, indicating whether the message has been retrieved by the recipient, has been opened by the recipient, is urgent and has an attachment;

Figure 12 is a schematic diagram of a menu indicating the formation of a network from a plurality of static resource groups and the revision of the composition of the network by the addition of groups and individuals to, and the deletion of groups and individuals from the network;

Figure 13 is a schematic diagram illustrating the different operations that can be performed by a user after the user has been invited to join a network; and

Figure 14 is a schematic diagram illustrating how the visibility of a message within a network providing the message and within other networks can be limited by a visibility manager so that only specific groups in the network providing the message and in other networks can see the message.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

Figure 1 is a schematic block diagram showing the inter-relationship between hubs and spokes in a public safety activity constituting a preferred embodiment of the invention. In Figure 1, a plurality of Radix hubs 10, 12, 14, etc. are shown at different geographical positions in the United States. Although a number of Radix hubs are shown, it will be appreciated that a number of additional Radix hubs may be provided and that these hubs may be provided at strategic positions throughout the United States. Generally, a hub may be provided to represent a relatively large area such as a state.

Hubs are constructed to communicate with one another as indicated by bold lines in Figure 1. For example, the California State Patrol may constitute a hub and the Los Angeles Police Department may constitute a spoke. Spokes are associated with an individual one of the hubs and are constructed to communicate with the associated hub. For example, spokes 16, 18 and 20 may communicate with the hub 10 and with one another. The communications between the spokes and the associated hubs is indicated by lines in Figure 1.

A plurality of spokes are provided to communicate with one another. For example, spokes 22 and 24 may communicate with the hub 12 and with each other. If the hub 12 wishes to communicate with any of the spokes 16, 18 and 20, the hub communicates directly with the spokes. However, if the hub 12 wishes to communicate with the spokes 16, 18 and 20, the hub 12 has to communicate with the hub 10 which then communicates with the spokes 16, 18 and 20. Each of the Radix spokes has different forms of communications available. For example, the Radix spoke 16 may illustratively communicate in Figure 2 by wireless with a laptop computer 26 and a handheld computer 28 and may communicate in a direct interface protocol connection with a workstation 30 in Figure 2.

Figure 3 is a block diagram schematically illustrating on a simplified block diagram basis, generally indicated at 34, the passage of information between several different agencies 36, 38 and 40 and a Radix hub 42. Each of the agencies 36, 38 and 40 may be governmental agencies such as agencies involving public safety activity. The agencies 36, 38 and 40 communicate with one another through the Radix hub 42. All of these interfaces are standard, allowing quick, seamless network integration.

The agency 36 may provide or receive information which is not secured and encrypted. This information is provided through a Radix switch 44. The agency 36 may provide information to the Radix switch 44 as from a satellite transceiver 48. The satellite transceiver 48 may communicate with, or receive information from, clients 50 (e.g., laptop computers, mobile data terminals, handheld devices, workstations.) The information at the Radix switch 44 may pass through a firewall 52 which encrypts the information before passing it to the Radix hub 42 from the agency 36 or passing information to the agency 36 from the Radix hub.

In like manner, the agency 38 may pass information to the Radix hub 42 through a Radix switch 53 or pass information from the Radix hub to the agency through the Radix switch. The agency 38 may include a radio frequency transmitter 54 and clients 56 corresponding to the clients 50. A firewall 58 providing an encryption may be disposed between the Radix switch 53 and the Radix hub 42. The Agency 40 may include a Radix switch 60, clients 62 and a firewall 64 corresponding respectively to the Radix switch 52, the clients 56 and the firewall 58. The agency 40 may have a different type of transceiver than the satellite transceiver 48 and the radio frequency transceiver 54. In addition to communication with the transceivers 48 and 54 and the transceiver associated with the agency 40, the Radix hub 42 may communicate with other Radix hubs.

The hub and spoke approach shown in Figures 1-3 and described above allows individual public safety agencies to select specific client applications and interface those applications with a local Radix message switch. In this way, agencies can leverage their own and other agencies' records and communications

infrastructures while maintaining the flexibility to use preferred client applications. The Radix message switch seamlessly integrates with existing network components both in hub and spoke permutations. In both permutations, the Radix message switch functions independently from other network components.

The advantages of a Radix-to-Radix communications path and a central hub are numerous and include:

a) one Radix switch can query a database stored in another Radix system; and

b) individuals can subscribe to different user resource groups, which makes them eligible for infant messaging communication or broadcast messaging. For example, agency A might have a group and agency B might have a group but both are members of a larger group. Messages addressed to the larger group will be forwarded to the individual members of sub resource groups recursively.

Figure 5 is a schematic diagram illustrating the relationship between a hub and spokes in an incident that occurred on Highway 287 in Colorado. Figure 5 includes a Colorado hub 70 and a pair of spokes indicated generally at 72 and 74. The spokes 72 and 74 are shown as being connected to the hub 70. The spoke 72 includes a Lafayette consolidated Radix switch which is connected to users including the Boulder Sheriff's Office 76, the hub, the Lafayette Police Department 78 and the Longmont Police Department 80. Included within these users are organizations designated in the lower left corner as Lafayette Consortium Message Resource groups. They constitute various police departments in Boulder and Longmont.

The spoke 74 constitutes a Douglas County Sheriff's Office Radix switch having a plurality of users designated in the lower left corner of a block as DCSO Message Resource groups. They include various Douglas County Police Departments and the Cunningham Fire Chief.

The organizations within the hub 70 are listed in a block 84. These include the Douglas County Sheriff's Office, the Boulder County Sheriff's Office, the

Longmont Police Department, the Lafayette Police Department and the Cunningham Fire District. All of these organizations constitute static resource groups because they exist as organizations and not as individuals and because they continue to exist as the individuals within the groups change. Also listed is a Dynamic Response Group formed from individuals within the static resource groups specified above. Communications are made directly to the individuals within the response groups. The individuals within the response groups facilitate the communications between the different resource groups in the network.

Figure 5 is based on an incident which occurred on U.S. Highway 287 in Colorado. It indicates a network which is formed of resource groups including the Douglas Country Sheriff's Office, the Boulder County Sheriff's Office, the Longmont Police Department and the Lafayette Police Department. All of these resource groups may be under the control of the hub 70 constituting the State of Colorado. All of the spokes may be invited by the hub group to join the network and become resource groups. When invited, the spokes have the option of accepting or declining the invitation. The spokes also have the option of inviting themselves as resource groups into the network. This self-invitation may be accepted or denied by the other resource groups in the network. The network includes resource groups which can contribute to the activity of the network. Each resource group can resign at any time from the network.

Each of the resource groups may have departments which are included in the resource group. For example, the Douglas County Sheriff's Office may include the Douglas County Sheriff's Office (DCSO) Patrol Group, the DCSO Haz-Mat Group, the DCSO SWAT Group and the DCSO Command Group. The spokes and the Departments in the networks are impersonal and static. In other words, they continue to exist even though the personnel in the resource group and the departments within the resource group change.

In addition to static resource groups in the network, there are also dynamic response groups in the network. The dynamic response groups are formed from individuals in the different resource groups in the network. For example, a dynamic

response group in Figure 5 may provide Highway 287 traffic control. It may include individuals from different resource groups in the network shown in Figure 5. John Doe and Longmont officers are indicated as being in the dynamic response group in Figure 5. The individuals in the dynamic response group are chosen by invitation and are included in the dynamic response group when they accept the invitation. Alternatively, the individuals may volunteer to be in the dynamic response group. They are included in the dynamic response group when their offer to volunteer is accepted.

Each individual in the dynamic response group may resign at any time from the dynamic response group. Alternatively, they may be removed by the dynamic response group from the network by a notification to them that they have been removed from the dynamic response group. The dynamic response groups are advantageous because they are generally formed of individuals who are interested in actively participating in the network as individuals in addition to performing work as members of static resource groups in the network.

The network shown in Figure 5 and described above has certain advantages. It provides the different resource and response groups in the network with up-to-date information. This allows each resource group and each response group to act independently in contributing to the public safety activity. It also allows the different static resource groups and the individuals in the dynamic response groups to act on a coordinated basis in dealing with the public safety activity. Another advantage is that the network is flexible because the messages can be constantly updated and different static resource groups and dynamic response groups can be included in the network and dropped from the network as the functions of the network change. Furthermore, individuals in the dynamic response group can be added or deleted from the dynamic response group as the functions of the dynamic response change with time. Furthermore, any messages can be transmitted by each individual or group in the network to any other group or individual in the network or to all of the groups and individuals in the network as the conditions change and warrant.

Each individual in a dynamic response group can be considered to act (1) in an individual capacity or (2) as a representative of the static response group of which he or she is a member or (3) in an individual capacity and as a representative of a static response group of which he or she is a member. The dynamic response group can accordingly be considered as being formed from individuals or from static resource groups or from a combination of individuals and static resource groups.

Figures 4a and 4b are alternative views, primarily in block form, of a Radix switch generally indicated at 90. Two alternative views are provided, primarily in block form, because of applicants' belief that they provide alternative viewpoints toward providing a full understanding of the construction and operation of the switch. The Radix switch 90 in Figures 4a and 4b corresponds in construction and operation to the Radix switches 44, 53 and 60 in Figure 3. In each of Figures 4a and 4b, signals are introduced to the Radix switch 90 from a selective one of the satellite transmitter 48, the radio frequency transmitter 54, a local area network 92 and a wireless client 94. These different transducers are exemplary of the different types of transducers that can be used. The signals are then introduced to a communications layer 95 which operates upon the signals to make the signals compatible with the Radix switch 90.

The signals then pass through a gateway 96 which is included in the Radix switch 90. The gateway 96 makes such determinations as: (a) who sent the message, (b) who will be receiving the message and (c) what are the contents of the message. The gateway 96 also determines from the contents whether the message is a request that requires a response. The Radix gateway 96 serves as the entry point for all client applications based upon Transmission Control Protocol (TCP) and internet Protocol (IP). The Radix Gateway 96 is further based on all client applications handling all Input/Output operations and connection management. The gateway 90 also provides security for the Radix switch by managing all user log-on validations. The gateway 90 handles all log-on, log-off, registration and de-

registration transactions. The gateway 90 is further responsible for passing incoming requests from a client to the remainder of the Radix system.

The Radix switch 90 also includes a message processing unit 98. The message processing unit 98 processes all messages and requests that pass to it from the gateway 96. The message processing unit 98 also parses the messages and requests. The message processing unit 98 then passes the processed and pared messages and requests to a system processing unit 100 which passes the message to the proper one of a plurality of backend systems. The backend systems may include (a) various databases 102, (b) systems 104 including a computer aided dispatch (CAD) system, a record management system (RMS), a department of motor vehicles (DMV) system and other external systems and (c) systems 106 including an all points bulletin (APB) system and an amber alert system.

The backend system may send messages, and responses to requests, back to the transmitters such as the satellite 54, the radio frequency antenna 48 , the local area network 92 and the wireless client 94. The messages and responses pass initially through the system processing unit 100. The system processing unit 100 provides substantially the same functions in the reverse direction that the gateway 96 provides in the forward direction. For example, the system processing unit determines who sent the message or response, who is to receive the message or response and what the contents of the message or response are. The system processing unit 100 is further responsible for directing the messages or responses to the recipient.

The message processing unit 98 operates upon the signals from the system processing unit 100 in substantially the same way in the reverse direction as it operates upon the signals from the gateway 96 in the forward direction. The message processing unit then passes the messages and responses to the gateway 94 which operates upon the message and responses in the reverse direction in substantially the same way as the system processing unit 100 operates upon the signals from the message processing unit 98 in the forward direction. The signals then pass through the communications layer 95 to the selective one of the satellite

transceiver 48, the radio frequency transceiver 54, the local area network 92 and the wireless client 94.

Figure 4b shows the Radix switch in additional detail. It shows that the message or request from the communications layer 95 passes to a client manager 110 which determines such parameters as who sent the message or request, who receives the message or request, and what the contents of the message or request are. The message or request then passes to a raw message or request 112 which provides a database for storing the message or request. The raw message or request 112 then passes to a process request manager 114 in the message processing unit 98. The process request manager 114 parses and formats the message or request as a formatted request 115 and directs the message or request to a request delivery manager 116 in the system processing unit 100. The request delivery manager 116 queues the message or request to the selective one of the backend units 102, 104 and 106. It also decides what adaptors 118 should be used to make the message or request compatible with the selective one of the backend units 102, 104 and 106.

The responses from the selective one of the backend units 102, 104 and 106 pass through the adaptors 118 to the request delivery manager 116. The request delivery manager performs substantially the same functions in the reverse direction as the client manager 110 in the forward direction. The response then passes from the request delivery manager 116 to a raw response 120 which corresponds in operation in the reverse direction to the raw request 112 in the forward direction. The response is then introduced to a process response manager 122 in the message processing unit 98. The process response manager 122 performs substantially the same operations on the response in the reverse direction as the process request manager 114 performs on the message or request in the forward direction. This includes parsing and formatting the response. The response then passes the parsed and formatted response to the client manager 110 which introduces the response to the communications layer 95 for passage to the selective one of the satellite transceiver 48, the radio frequency transceiver 54, the local area network 92 and the wireless client 94.

Figure 4a includes certain additional blocks. For example, a security manager 126 is included in the gateway 96. Users have to log into the network. The security manager 126 checks the security of these users. The functions of a performance manager 128 are extended across the gateway 96, the message processing unit 98 and the system processing unit 100. The performance manager 128 redirects messages, requests and responses to the proper places in both directions and monitors all of the messages, requests and responses. The performance manager 128 provides solicited and unsolicited messages, requests, and responses concerning the Radix system 90 and the use of its resources. The performance manager 128 produces notification messages when a software error occurs and when traffic thresholds are reached. The performance manager 128 can also reset statistics or disable the gathering of statistics. Performance manager configurations can be dynamically updated by using a Radix Administration Tool 132 without affecting the performance of the Radix switch.

A block 130 designated as "Request/Response Monitoring" is shown in Figures 4a and 4b. This block indicates that a supervisor can watch messages, requests and responses as they pass through the Radix switch. The request/response monitoring component 130 generates statistical information concerning daily inquiries and responses. Reports specifying the daily usage of the Radix switch, the number of requests and responses, and other database-specific usage statistics are accessible through this component.

Requests for statistical information from the Radix Administrative Tool 132 come through the switch interface module and then pass to the request and response monitor 130. The request and response monitor 130 uses the query module to retrieve message information from databases. The request and response monitor 130 can format results into a report of hourly statistics over a 24-hour period. This report is then passed to the switch interface module and is routed to the component that made the report request. The Radix Administration Tool 132 provides a user interface for a Radix configuration. The Tool 132 may be browser-based. The Tool 132 allows administrators to modify a live Radix system dynamically. The

Tool 132 manages the entire Radix system. This management includes tasks such as user configuration, setting timeout lengths and editing configuration files. The Radix Administration Tool 132 allows the administrator to modify the Radix system remotely.

To facilitate system analysis, the Radix switch 90 includes an archiving component 134 to log all of the traffic processed. A Radix System Administrator can configure the archiving component to certain thresholds and to specified information. Client requests, backend system response, system errors and system events are a few of the data that can be archived. The system administrator can specify the length of time that any of the logs remain in the system. Time stamps are stored with every type of data that the archiving component stores. For all requests and responses to or from users, the user identification is stored with the associated log.

Figure 6 provides a window 131 indicating a user tree relating to the public safety activity. The leftmost pane 133 in the window 131 shows the static resource groups and dynamic response groups in the network. When an item in this tree is displayed by a first color (e.g. green), it indicates that the resource group or the response group or the individual in the response group is currently online and connected in the network. When displayed in a second color such as grey, the group or individual is not currently online. Portions of the user tree may be expanded by activating a (+) button 35 adjacent that portion or may be contracted by activating a (-) button 137 adjacent that portion of the user tree.

Each group and individual may be selected as a recipient for a message, request or response by providing a single click on the name of the user or may be deselected by providing a double click on the name of the group or individual. When a group or individual is selected as a recipient of a message, a request or response, an "x" notation will be provided next to that party's name.

An "in" box 139 is provided to the right of the list of resource groups and response groups. The in-box 139 includes in separate lines the names of the resource groups and the individuals and the subject matter of the message, request

or response. The in-box 139 also includes the data and time that the message, request or response was received. Each in-box 139 also includes an envelope icon 134. An open envelope icon 134 indicates that the message, request or response has been read. A closed envelope icon 134 indicates that the message, request or response has not been read. A message may have a high priority as indicated by an exclamation mark 141 to the left of the name of the group or individual. A paper clip 136 adjacent the portion of the indication of high priority indicates that there is an attachment to the message, request or response.

Figures 6 and 7 indicate a number of different buttons that can be individually operated in a control panel to provide different operations for managing the messages, requests or responses in the Radix switch. A first button is designated as "refresh" and is indicated at 138. The actuation of this button provides for an updated indication of the user tree and provides for an indication of the current status of the static resource groups, departments in the static resource groups, dynamic response groups and individuals in the response groups. A button 140 designated as "groups" is available to be actuated by a resource group or response group if the system administrator has provided the resource group or the response group with authority to create and manage a dynamic response group. Once clicked, it displays a menu that allows the resource group or the response group to create a new dynamic response group, invite users to an existing dynamic response group and perform other management tasks related to the dynamic response groups.

When actuated, a "delete" button 142 will cause a selected message to be deleted from the "inbox" of the resource group, response group or individual. A "forward" button 144 provides for a forwarding of a selected message, request or response from the inbox of the forwarder to the other users when the button is actuated. The message, request or response will go only to those who have been selected as recipients in the user box of the forwarder. This is indicated by an "X" adjacent the name of the recipient in the user tree. The message remains in the inbox of the forwarder when it is forwarded to the recipients.

A "reply" button 146 is clicked at the "inbox" of the recipient to send a response from the recipient to the sender of a selected message or response from the sender to the recipient. The response goes only to the sender and does not go to any other users who or which have received the message from the sender. A "reply all" button 148 provides for the message or response to be sent from the recipient to the sender and to all other users who have received the message. An "export" button 150 provides for an export of a selected message, request or response as a text file. The file can be saved to any location on a hard drive and/or network where the file has read/write permission. The format of the selected message, request or response in the file is plain ASCII text and can be viewed with Windows Notepad or imported into any word processor or text editor.

When actuated, a "save" button 152 allows a selected message to be saved in the user's machine. This will allow the message, request or response to be viewed later even when other messages cannot be retrieved from the user's machine. When a "read" button 154 is actuated and a new, unread message, request or response is selected, the contents of the message, request or response will be retrieved and displayed in the lower panel of the inbox to be read. When a message, request or response has not yet been read or retrieved from the server, a message reading "click <read> to retrieve this message from server and view it" is provided in the message content pane. When a message, request or response has already been retrieved and requested and is subsequently selected and a "Set New" button 156 is activated, the status of the selected message, request or response will be changed to "new". In doing so, the envelope icon 134 for the selected message, request or response will be changed from an opened envelope to a closed envelope.

Figure 8 shows how a message, request or response is generated. If a sender can view an entry for a recipient in the sender's inbox, the sender can send the recipient the message, request or response. To send a message, the sender first clicks the "new" tab at the top of the inbox as shown at 160 in Figure 8. This changes the inbox portion of the screen to look like Figure 8. To compose a message, the sender provides a subject 162 for the message text into the large area

provided in Figure 7 for the text. If the message is a high priority message, the sender clicks the urgent checkbox 164 at the bottom right of the message area. When an urgent message is received by a recipient, it is indicated by the large exclamation mark 141 in Figure 6.

If the sender wishes to recompose the message, the sender operates the "clear" button 166 at the bottom left of the inbox. The sender can then recompose the message, request or response in the box. The sender has three (3) options in sending messages, requests or responses to members of the network. These are as follows: (a) group all members of the group and all departments in the group, (b) members of the group who are online and connected to the Radix, as indicated by their name being printed in green text as distinguished from members who are offline and are indicated in a gray text, and (c) all members of a group regardless of their online status. Each of these options can be selected by double-clicking that option. The (x) notation is displayed adjacent each of the selected groups to indicate that the group has bee selected. When the message, request or response has been completed and the receiving group has been selected, a "send" button 168 in Figure 8 is actuated to send the message, request or response. Attachments to the message are provided as indicated at 136 in Figure 6.

As previously indicated, attachments can be provided for messages, requests and responses. To choose a file from a machine as an attachment, a browse button 170 in Figure 9 is actuated. This provides for a file to be selected from the sender's local or network drives. Files selected will be listed in the list box 172 shown in Figure 9. This list box is identified in Figure 9 as "c:\files\blueprints.bmp". To remove a file from the message, request or response before the message, request or response is sent, the file is checked and then a delete button 174 is clicked. The area 176 to the right of the list box 172 is provided to view attachments before the message and the attachments are sent. The "connect" box 178 is used to connect any image capture device (e.g., digital cameras, scanners, etc.) that may be connected to the sender's system.

Figure 10 is a diagram showing how a message, request or response is viewed at a recipient. As indicated in Figure 10, various types of information are provided in a line on the recipient's screen. For example, the name of the recipient is indicated at 180 in Figure 10. If the message hasn't yet been retrieved by the recipient, a green check mark 182 is not provided and the "read" button will have to be actuated to retrieve the message, request or response. Once retrieved, the bottom portion of the inbox pane will display the text of the message, request or response and a list of the recipients.

If there are any attachments to the message being viewed, there will be an "attachments" tab 184 similar to that indicated at 136 in Figure 6. To view or save the attachment, the "retrieve" button 182 is actuated. This causes the attachment to be displayed at the right portion in Figure 9. Once an attachment has been retrieved and displayed, the green checkmark 182 will be displayed next to its name as indicated in Figure 9. As indicated at 181 in Figure 6, the message subject is displayed. If the message is urgent, this is indicated by an exclamation mark 183. This corresponds to the exclamation mark 141 in Figure 6. An indication is provided at 185 of the date and time that the message is sent.

One of the most useful features of the system and method constituting this invention is the ability to create a network composed of resource and response groups on an almost instantaneous basis. The inclusion of the static resource groups and the dynamic response groups and the individuals in the response groups is dependent upon the problems that the network will face based upon incidents or conditions that require unique communications among the groups and individuals in the network. The inclusion of the group and the individuals in the network may vary with time as the problems faced by the network and the characteristics of the incident change with time.

Figure 11 indicates how a network is created and how it is varied with time. To create a network, a button 188 designated as "groups" is actuated to create a small menu indicated in Figure 11. The button 188 can be actuated only by groups given prior authorization. To create a response group, a button 190 designated as

"create a response group" is actuated. A button 192 designated as "invited selected users to a response group" is then actuated. The users (resource groups, response groups, individuals) are then selected. An "OK" button 194 is thereafter clicked and the selected group and individuals will appear at the appropriate positions in the network. Each selected group and individual will receive an invitation to join the network. All of the selected groups and individuals can be invited simultaneously or the selected groups and individuals can be invited individually. As they accept, they will appear at the appropriate positions in the network. When it is desired to delete a resource group or a response group from the network, the group or individual is selected in the same way as for an invitation. A button 196 designated as "delete selected user from response group" is then actuated. It will be appreciated that only designated users are authorized to delete previously selected groups and individuals from a network.

Figure 12 indicates how a group or an individual responds after receiving an invitation to join a network. When a group or individual receives an invitation, the group or individual accepts the invitation by actuating an "accept" button 200 at the bottom of the message window. The group or individual declines the invitation by actuating a "delete" button 202 at the bottom of the messaging window. This is done in accordance with the invitation that is provided in the messaging window.

Figure 13 is a diagram schematically showing on a fragmentary basis the interoperability of a user 210 constituting an administrator, a user 212 constituting an individual using the system of this invention in the field and a Radix server 214 in passing messages and other information from one to another. Figure 13 is only exemplary of what can be accomplished by the system of this invention. It is not intended to be limiting in any way. It is believed that the Figure is self-explanatory in view of the information specified in each of the ovals and in view of the prior discussion.

Figure 14 shows a system in block form for controlling the promulgation and publication of messages in different networks. A visibility manager 240 is indicated in Figure 14 for managing the publish/subscribe relationships of different

networks. These are indicated in Figure 14 as networks or organizations A, B and C. Network A publishes its messages, requests or responses from Group A in network A to network B; network A publishes its messages, requests and responses from group A2 in network A to networks B and C; and network A publishes its messages, requests and responses from group A3 in network A to network C. Network A can see the publications in group B1 in network B and group C2 in network C. This is illustrative of what networks B and C can respectively publish and see. Similar indications are provided for networks B and C of what each of networks B and C can publish and promulgate and can see.

Although this invention has been disclosed and illustrated with reference to particular embodiments, the principles involved are susceptible for use in numerous other embodiments which will be apparent to persons of ordinary skill in the art. The invention is, therefore, to be limited only as indicated by the scope of the appended claims.